UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,681	12/08/2003	Joon-Kit Goh	SE0039	5707

29393 7590 07/18/2008
ESCHWEILER & ASSOCIATES, LLC
NATIONAL CITY BANK BUILDING
629 EUCLID AVE., SUITE 1000
CLEVELAND, OH 44114

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

NOTIFICATION DATE	DELIVERY MODE
07/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing@eschweilerlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/730,681	GOH, JOON-KIT	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2008 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on May 01, 2008 has been entered. Claims 1, 3-26 are pending. Claims 27-32, 34 are canceled by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3, 4, 6, 9-21, 23, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qi et al (US Patent No. 7,142,671) and in view of Anand (US Patent No. 7,280,657).

As per claim 1, Qi teaches: the DES engine having a message input, a cipher key input, and a pre-data output, the engine adapted to receive and selectively process a block of data from the message input of the security processing circuit during a first DES processing operation, and subsequently to process data from an intermediate result during second and third DES processing operations and store an intermediate result of the third DES processing operation to the pre-data output [Fig. 4A, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-14]; a security keys circuit having a set of cipher keys input and a key output, the security keys circuit operable to select and transfer a

different cipher key to the key output coupled to the cipher key input of the DES engine selected from the set of cipher keys associated with each DES processing operation during the first, second and third DES processing operations [Fig. 4A – 419 col. 8 lines 29-64]; and a data output circuit having a pre-data input and a data output, the pre-data input of the data output circuit coupled to the pre-data output of the DES engine, and the data output selectively coupleable to the host system, the data output circuit operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A, 1, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-14], wherein the DES engine comprises: a permutation block having the message input and a permutation output, the permutation block operable to receive a block of data at the message input and to perform an initial permutation of the message input data and provide a permutation result at the permutation output [Fig. 4A, 4B, 5, col. 7 lines 6-29, col. 9 lines 15-19]; a data input multiplexer having a first and second input and a data selection output, the data input multiplexer operable to select and couple one of the first and second inputs to the data selection output; an intermediate result register having a data input, a clock input, and a latched data output, the register operable to store fight and left half results of the initial permutation or of a cipher process based on data present at the data input upon receipt of a clock signal at the clock input; a pre-data output multiplexer having a first and second input and a data selection output, the pre-data output multiplexer operable to select and couple one of the first and second inputs

to the data selection output [Fig. 4A,4B]; and a pre-data output register having a data input, a clock input, and a latched data output [Fig. 4A, 4B], wherein the permutation output of the permutation block is coupled to the first input of the data input multiplexer, the data selection output of the data input multiplexer coupled to the data input of the intermediate result register, the latched data output of the intermediate result register coupled to the data input of the cipher blocks having the cipher output of the cipher blocks feedback coupled to the second input of the data input multiplexer and to the first input of the pre-data output multiplexer the data selection output of the pre-data output multiplexer coupled to the pre-data output register, the latched data output of the pre-data output register feedback coupled to the second input of the pre-data output multiplexer and the pre-data output [Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32].

Qi teaches cipher block for performing the ciphering process and providing the result to the intermediate register as above.

Anand teaches: eight cipher blocks having a data input, a key input, and a cipher output, operable to receive data at the data input and a key at the key input, to perform the cipher process comprising right and left halves of cipher process on the data at the data input employing the key, and to provide a first and second cipher result cycle of each of the three DES processing operations [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Anand with Qi, since one would have been

motivated to increase the security or to make a cipher stronger and perform the encryption and decryption in less time [Anand, col.2 lines 3-5, 35-41].

As per claim 3, the rejection of claim 2 is incorporated and Qi discloses:

wherein the DES engine is further operable to perform the initial permutation of the message input data using the permutation block, initially select the permutation result with the data input multiplexer and couple and store the result to the intermediate result register during a data input latch cycle, to transfer the initial result and the cipher key from the security keys circuit to the cipher blocks for cipher processing and intermediate storage of the right and left halves of the first step cipher results subsequent to selection of the second input of the data input multiplexer into the intermediate result register during the first cipher process cycle, to transfer the stored intermediate result and the cipher key from the security keys circuit to the cipher blocks for cipher processing and intermediate storage of the right and left halves of the second step cipher results subsequent to selection of the second input of the data input multiplexer into the intermediate result register and the pre-data output register subsequent to selection of the first input of the pre-data output multiplexer during the second cipher process cycle of the first DES processing operation, and wherein the DES engine is operable to repeat the first and second cipher process cycles for the subsequent second and third DES security processing operations of the security processing circuit [Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32], and latch the intermediate result of the third DES operation to the pre-data

output of the pre-data output register of the DES engine, using the selection of the second input of the pre-data output multiplexer during the third DES processing operation of the 3DES security processing [Fig. 4A, 4B, col. 8 lines 44-67-col. 9 lines 1-14].

Anand teaches eight cipher blocks for cipher processing [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

As per claim 4, the rejection of claim 3 is incorporated and Qi discloses: wherein the 3DES processing is completed in three single DES processing operations [col. 5 lines 35-42, col. 8 lines 65-67].

As per claim 6, the rejection of claim 3 is incorporated and Anand discloses: Wherein the first, second and third DES processing operations each have a duration of two clock cycles [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

As per claim 9, the rejection of claim 1 is incorporated and Qi discloses: coupled to one or more of the DES engine, the security keys circuit, and the data output circuit for timing clock cycles of the first, second and third DES processing operations of the 3DES processing for the security processing circuit [Fig. 4A, 4B, 5].

As per claim 10, the rejection of claim 1 is incorporated and Qi discloses:

a set of cipher keys input, wherein the set of cipher keys comprise three different cipher keys, each cipher key associated with one of the three DES processing operations of the 3DES security processing [Fig. 4A]; a keys input multiplexer having a set of cipher keys input, and a cipher key selection output, the keys input multiplexer operable to select and couple a cipher key to the cipher key selection output [Fig. 4A]; and a security keys register having a data input, a clock input, and a latched data output, the register operable to store the cipher key selection associated with one of the three DES processing operations of the 3DES security processing based on cipher key data at the data input upon receipt of a clock signal at the clock input, the latched data output of the security keys register coupled to the key input of the cipher blocks [Fig. 4A, col. 8 lines 29-67, col. 9 lines 1-14]. Anand teaches the eight cipher blocks [Fig. 2A].

As per claim 11, the rejection of claim 10 is incorporated and Qi discloses: the keys input multiplexer is operable to receive the three cipher keys and to selectively couple one of the three cipher keys associated with a DES processing operation to the DES engine during the three DES processing operations of the 3DES security process [Fig. 4A].

As per claim 12, the rejection of claim 1 is incorporated and Qi discloses: an inverse permutation block IPB having a pre-data input and an inverse permutation output, the block operable to receive and further security process the pre-data output from the DES engine, performing an inverse permutation of the pre-data

and transfer the processed data to the inverse permutation output [Fig. 4A, col. 9 lines 58-67, col. 10 lines 1-14]; an XOR gate XOR having a processed data input, an initialization vector input, and an XOR gate output, the XOR gate operable to selectively exclusive OR the initialization vector at the initialization vector input together with the processed data from the inverse permutation output of the inverse permutation block coupled to the processed data input, and transfer the XOR data to the XOR gate output [Fig. 4A, 4B, col. 8 lines 44-64]; a data output multiplexer having a first and second input, a selection control signal, and a data selection output, the data output multiplexer operable to select and couple one of the first and second inputs to the data selection output, based on the state of the selection control signal, the first input coupled to the XOR gate output, and the second input coupled to a data output register [Fig. 4A, 4B]; and the data output register having a data input, a clock input, and a latched data output, the register operable to store the output data results of the third DES process based on data present at the data input upon receipt of a clock Signal at the clock input, the latched data output of the data output register feedback coupled to the second input of the data output multiplexer to insure latching of the data at the output, wherein the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A, 4B, 5, col. 8 lines 44-67, col. 9 lines 1-14].

As per claim 13, the rejection of claim 12 is incorporated and Qi discloses: the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A].

As per claim 14, the rejection of claim 1 is incorporated and Qi discloses: wherein the security processing circuit resides within a network interface device of a host system for performing 3DES encryption and decryption services for the host system using a DES engine [Fig. 1, 4A, col. 3 lines 39-57].

As per claim 15, the rejection of claim 1 is incorporated and Qi discloses: a network interface device coupled with the security processing circuit, the network interface device being adapted to selectively encrypt outgoing data from the host system to cryptographically process data for transmission to the network [Fig. 1, 4A, 4B].

As per claim 16, the rejection of claim 15 is incorporated and Qi discloses: the network interface device comprises a bus interface, a media access control system, and the security processing circuit [Fig. 1].

As per claim 17, the rejection of claim 16 is incorporated and Qi discloses: the network interface device is a single integrated circuit [Fig. 1].

As per claim 18, the rejection of claim 1 is incorporated and Qi discloses: the circuit comprises an IPsec circuit adapted to selectively provide authentication, encryption, and decryption functions for incoming and outgoing data [Fig. 1, 2].

As per claim 19, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 20, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

As per claim 21, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 23, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 26, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 9. Thus, it is rejected with the same rationale applied against claim 9 above.

3. Claims 5, 7, 8, 22, 24, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qi et al (US Patent No. 7,142,671) in view of Anand (US Patent No. 7,280,657) and in view of Callum (US Patent No. 6,985,581).

As per claim 5, the rejection of claim 3 is incorporated and Callum discloses:
wherein the 3DES processing is completed in eight clock cycles [Fig. 3 col. 2 lines 46-67, col. 3 lines 1-25].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Callum with Qi and Anand, since one would have been motivated to increase the security or to make a cipher stronger and perform the encryption and decryption in less time [Anand, col.2 lines 3-5, 35-41].

As per claim 7, the rejection of claim 3 is incorporated and Callum discloses: the clock cycle has a period of about 8ns [Fig. 3].

As per claim 8, the rejection of claim 5 is incorporated and Callum discloses: wherein the eight clock cycle of the 3DES security processing comprise: a data input latch cycle; a first DES processing operation comprising two cycles; a second DES processing

operation comprising two cycles; a third DES processing operation comprising two cycles; and a data output latch cycle [Fig. 3 col. 2 lines 46-67, col. 3 lines 1-25].

As per claim 22, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 24, the rejection of claim 22 is incorporated and it encompasses limitations that are similar to limitations of claim 7. Thus, it is rejected with the same rationale applied against claim 7 above.

As per claim 25, the rejection of claim 22 is incorporated and it encompasses limitations that are similar to limitations of claim 8. Thus, it is rejected with the same rationale applied against claim 8 above.

Response to Argument

4. Applicant's arguments filed May 01, 2008 have been fully considered but they are not persuasive.

Regarding to applicant's argument that neither Qi nor Anand teach "feedback coupled to the second input of the data input multiplexer and to the first input of a pre-data output multiplexer". Examiner maintains since, Qi's invention relates to

implementing a cryptography engine to perform cryptography algorithm such as a DES algorithm. The cryptography engine for performing cryptographic operations (such as DES, Triple DES) on a data block is provided. The cryptography engine includes a key scheduler configured to provide keys for cryptographic operations. As shown in fig. 2, the cryptographic processing unit comprising input/output buffer, cryptographic engine. The cryptographic engine contains surrounding logic and DES engine. DES engine includes asynchronous FIFO interfaces. Fig. 4a, represent the DES engine, which includes input FIFO to decouple the DES engine from surrounding logic. A 64-bit data block is combined with an initialization vector from initialization vector block. The 64-bit block then undergoes an initial permutation, before round 1. Two-level multiplexer stage contains four multiplexers for determining whether to load initial data, swap data from the previous round, or not swap data from the previous round. Initial data is loaded in the first round of DES processing. Data is swapped between rounds of DES processing. Data is not swapped in triple DES between the completed 16 rounds of DES processing Control logic can track the round number in order to determine what signals to send to the multiplexers. The first level multiplexers are sent a signal to load or not to load data from a previous round or to allow initial data to pass through after initial permutation. The expansion logic 415 changes the order of the bits in the 32-bit at block and also repeats certain bits. The expansion logic 415 uses the 32-bit block to generate a 48-bit block. The expansion logic improves the effectiveness of the encryption process and also makes the 32-bit block into a 48-bit block that corresponds to the size of the key. The 48-bit block can then be combined with an XOR with the 48-bit round key at 417.

Keys are provided by key generation logic or key scheduler circuitry 419. A version of the key for cryptography processing of the original 64-bit block is provided by key scheduler 419. Key scheduler 419 can provide a different version of the original key for every round by applying permutation and shift functions to all 56 bits of the original key. According to various embodiments <u>eight Sboxes are provided in Sbox stage 427</u>.The 32-bit output of Sbox stage is provided to permutation stage 429. A permutation stage 429 maps input bits in certain positions to different output positions. The 32-bit output of permutation stage 429 is combined with an XOR with the value in register 411 at 431. The result of the XOR is provided to the register 411 through multiplexer stage 409 for the next round of DES processing. That is, the right half is expanded, combined with an XOR function with a version of the key, provided to a Sbox stage, permuted, and combined with an XOR with the left half. After the last round, the outputs are written to register 433 and register 435. The output can then undergo a final permutation at 437. The result of a final permutation at 437 is combined by way of an XOR with an initialization vector as noted above when the DES engine is used to decrypt data. Otherwise, the result of the final permutation at 437 can remain unchanged by combining by way of an XOR with a sequence of zeros. For triple DES, the outputs at 433 and 435 are passed back to multiplexer stage 409. Control circuitry determines how to pass the data back to register 411 and 413 for a next 16 rounds of DES processing. Therefore, Qi teaches the DES engine/cryptography engine for performing 3DES operation as above. Further, in an analogous art, Anand's relates to the field of cryptography, in particular to block ciphering and to implementations of the triple data

encryption algorithm for the data encryption standard. As shown in Fig. 2, the cipher block portion 200 of system comprises initial cipher round block 260, a plurality of cipher round blocks 262, a final cipher block 266 and cipher output swapping block 268. The portion 200 is preferably implemented with either one, three, four, eight or sixteen cipher round blocks, each performing their cipher round operations preferably during one clock cycle. Since DES ciphering requires sixteen rounds of ciphering, one clock cycle is needed if sixteen cipher round blocks are implemented, two clock cycles are needed when eight cipher round blocks are implemented, four clock cycles are needed when four cipher round blocks are implemented, and six clock cycles are needed when three cipher round blocks are used. The cipher block portion 200 reduces the number of XOR operations in the critical timing path. The permuting function (Ef) operates on both the left input as well as the output from the permuting function (Pf). The output of left permuting function (Ef) (220) is XOR'ed (222) with the key producing an output which is stable in time much earlier than the S-box output. The critical timing path for each round of ciphering thus comprises the path through the S-box, the permuting function (Pf) and XOR gate (224), which is one less XOR gate that standard DES implementations. Therefore, Anand discloses <u>the improved cryptography engine for performing the DES operation by reducing time required for critical path operation</u> as above. In this case, the combination of Qi and Anand teaches the improved security processing circuit for performing 3DES operation as claimed. In fact, Qi and Anand do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in

structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations. In this case, even though the prior art Qi and Anand have different structure from the claimed invention but they perform the similar function and provide similar result as claimed and therefore, it meets the claim limitation.

For the above reasons, it is believed that the rejections should be sustained.

Terminal disclaimer has been filed on May 2, 2008 and therefore, the provisional double patenting rejection is withdrawn.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Adams et al (US 6031911) – Practical S Box design

Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
7/9/08
/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135